ISSN 2544-9338
INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGIES IN SOCIAL SCIENCE
RS Global
Scientific Edition

International Journal of Innovative Technologies in Social Science

e-ISSN: 2544-9435

Scholarly Publisher
RS Global Sp. z O.O.
ISNI: 0000 0004 8495 2390

Dolna 17, Warsaw,
Poland 00-773
+48 226 0 227 03
editorial_office@rsglobal.pl

ARTICLE TITLE	THE CYBERSPACE AND MILITARY MODERNIZATION: LEADERSHIP, TRAINING, AND HUMAN RESOURCE STRATEGY
DOI	https://doi.org/10.31435/ijitss.4(48).2025.4442
RECEIVED	27 October 2025
ACCEPTED	23 December 2025
PUBLISHED	30 December 2025
LICENSE	The article is licensed under a **Creative Commons Attribution 4.0 International License.**

THE CYBERSPACE AND MILITARY MODERNIZATION: LEADERSHIP, TRAINING, AND HUMAN RESOURCE STRATEGY

Khulan Dorjpalam
Lieutenant, Lecturer at the Cyber Security Department, Military Joint School, National Defense University, Mongolia

ABSTRACT

This article explores cyberspace as a new strategic domain made up of interconnected networks of information technology infrastructure and analyzes the changes taking place in the management, training, and human resource policies of the armed forces. The research utilizes theoretical analysis, international experiences, and comparative research methods, focusing on case studies from NATO, the United States, Germany, the United Kingdom, Russia, China, and Estonia. It discusses the theoretical perspective of considering cyberspace as a fifth conflict domain, cyber force structure and management reform, red/blue team training, and ongoing capability development trends.

The findings highlight that addressing cyberspace issues requires not only technical solutions but also a comprehensive modernization of strategy, organization, and human factors. This underscores the critical importance of developing human resource policies, management structures, and training systems in the defense sector as part of an integrated strategy.

Dedicated cyber forces have improved response times to cyber incidents, while enhanced training programs have bolstered cyber discipline and threat awareness among military personnel.

Effective cyber defense necessitates the development of human resource policies, management structures, and training systems within the defense sector as part of a cohesive strategy. The research emphasizes the need for a holistic ecosystem encompassing practical training, continuous capability development, flexible human resource policies, multidisciplinary expertise, and robust public-private partnerships to combat evolving cyber threats. Sustaining a competitive edge in cybersecurity requires ongoing adaptation and investment in technological infrastructure and human capital development.

KEYWORDS

Cybersecurity, Cyberspace, Cyber Warfare, Military Modernization, Cyber Command, Training Transformation, Human Resource Strategy

CITATION

Khulan Dorjpalam (2025) The Cyberspace and Military Modernization: Leadership, Training, and Human Resource Strategy. *International Journal of Innovative Technologies in Social Science*. 4(48). doi: 10.31435/ijitss.4(48).2025.4442

Introduction

As modern military operations have become more focused, the professional development of the armed forces is crucial for national security and international stability. Cyberspace has now become a new battleground, alongside land, sea, air, and space, adding a new layer to security geopolitics. A study examining changes in the cyber policy and budget of the US Armed Forces has highlighted information and communication technology as the key link in modern military operations, emphasizing the importance of cyberspace in all operational environments.

Cyberspace is not just a technological advancement, but also plays a crucial role in the country's defense capabilities and strategic balance through the rapid flow of data, data-driven decision-making, and network security. This has led to conflicts and wars being fought in the realm of digital information rather than traditional weapons. However, there is still a lack of consensus on the terminology and definition of "cyberspace" as a strategic domain. The term "cyber" is interpreted differently by various stakeholders, with some focusing on computers, networks, and information security, while others view it as a broader space encompassing all forms of information, electromagnetic waves, and user behavior. This diversity of perspectives creates challenges in developing policies and programs related to “cyber security,” “cyber defense,” and “cyber warfare.”

Cyber conflict can take various forms, including low-intensity attacks like cybercrime, espionage, and service disruption, as well as full-scale warfare that incorporates cyberspace in armed conflict.

Hence, cyberspace has evolved into more than just a “contextual environment for war preparations,” but a strategic arena that spans all stages of peacetime, crisis, and war. Spidaleri and McArdle highlight that persistent low-intensity cyberattacks and incursions place a constant strain on the day-to-day operations of peacetime military forces, necessitating educational institutions that train defense personnel to develop a training regimen that aligns with the unique characteristics of the cyber domain.

As such, this article systematically explores the interplay between cyberspace, cyberwarfare, cyber military leadership, and emerging training practices.

Cyberspace: A New Domain for Military Operations and International Practices

Cyberspace is a virtual, non-physical environment within the information realm that can have significant real-world consequences. It encompasses a complex network of information systems and devices, including the Internet, telecommunications infrastructure, and computer networks, which are essential for various aspects of society such as business, finance, government, and military operations. Unlike traditional physical boundaries, cyberspace transcends geographical borders, allowing attackers to impact a country's security and development by disrupting critical infrastructure, services, and information. As a result, many nations view activities in cyberspace as a matter of national security. NATO's recognition of cyberspace as a new domain for military operations enables member states to respond to cyber-attacks as they would to physical military threats, emphasizing the importance of enhancing cyber defense capabilities at a strategic level to safeguard sovereignty and independence.

Traditional military theory has long recognized land, sea, and air as the main battlefields, with space later added. However, in the information age, cyberspace has emerged as the fifth (and sometimes sixth) battlefield. The US Department of Defense's 2011 Cyber Strategy defined cyberspace as a distinct domain for military operations, emphasizing the need for specialized military forces to be organized, trained, and equipped. This strategy has served as a foundational document guiding efforts in this direction. Russia, on the other hand, has elevated the struggle in the information space to a theoretical level, encompassing cyber operations within the concept of “information warfare.” As a result, operations in cyberspace have become an essential component of modern military missions, on par with traditional domains. Terms like cyber warfare, information warfare, and network warfare are now commonly discussed in the context of multi-domain operations, reflecting their strategic significance.

Each country is exploring different structural and organizational approaches to safeguard and leverage advantages in cyberspace. International practices reveal two primary trends in cyber force management and organization. Firstly, the creation of an independent cyber force and command: Germany established the Cyber and Information Space Command in 2017, elevating it to the same level as its land, sea, and air forces. Initially comprising a small group of IT experts, the command aims to expand to include tens of thousands of military personnel and civilians, underscoring its recognition of cyberspace as a distinct strategic domain. Russia formed an information warfare and cyber operations force to defend its information systems from external threats and conduct offensive cyber activities. China initially integrated cyber, space, and electronic warfare under the Strategic Support Force in 2015 but later restructured in 2024 to create a dedicated cyber military force responsible for offensive and defensive cyber operations as well as intelligence tasks. Secondly, the integrated joint cyber command model: The United States established USCYBERCOM within the Strategic Command in 2009, elevating it to an independent command in 2018 to oversee cyber capabilities across all military branches. Cyber commands within the army, navy, and air force report to USCYBERCOM, playing a pivotal role in various operational domains. Estonia operates a voluntary Cyber Defense Unit, employing a state-civilian partnership model for cyber defense. The UK's National Cyber Force, a collaborative initiative between the Ministry of Defense and GCHQ, exemplifies a civil-military joint approach to offensive cyber operations.

Cyber warfare differs from traditional warfare in the following key ways:

- Traditional warfare is fought over physical boundaries on land, water, and in the air, while cyber warfare is fought over cyberspace without regard to physical boundaries. Cyber warfare does not have clear battle lines like traditional warfare.

- Even a small amount of direct physical destruction in traditional warfare can lead to hidden damage, such as financial, energy, medical, and communications disruptions, as well as secondary human lives and social unrest.
- Traditional warfare is formally declared and follows a certain cycle, while cyber warfare is a continuous and ongoing effort to infiltrate and engage in combat, blurring the lines between peacetime and wartime.
- Identifying and holding perpetrators accountable in cyber warfare is technically and legally challenging.
- Cyber-attacks can target multiple locations worldwide in seconds or minutes, requiring defenders to make near real-time decisions.

These features show that traditional strategies and tactics cannot simply be replicated, and that new theories, procedures, and training methods are necessary to address the unique challenges of the cyber environment. Military leaders and staff officers are adapting by developing new knowledge and tactics to achieve dominance and thwart cyber-attacks, leading to a reevaluation of traditional war doctrines. Nations like the United States, Japan, and Korea are integrating cyber warfare theory and practice into their military academies and training programs in response to the rapid advancement of information technology.

The rapid increase in cyber threats is leading to new trends in military training and personnel development. As a result, defense organizations worldwide are updating their cyber training programs and following specific directions. One key trend is the use of simulations and exercises based on real-world scenarios, with practical training in real cyber situations taking precedence over theoretical instruction. For instance, Keepnet Labs conducts exercises where soldiers receive simulated emails from their commander to test their susceptibility to phishing attacks and learn from any errors. Additionally, red team/blue team attack-defense drills and collaborative training on NATO's Cyber Range are now the primary methods for honing skills in realistic settings.

Secondly, the trend towards advanced continuous training is gaining traction. Given the ever-evolving nature of cyber technologies and tactics, it is no longer sufficient to rely on a single training session. As a result, the United States has implemented a system of flexible modular training and continuous professional development pathways. Additionally, a center for advanced cyber education has been established to support the sustainable growth of skilled personnel.

Thirdly, a robust human resources policy is crucial for recruiting and retaining cyber specialists in the military. To prevent the loss of highly skilled personnel to the private sector, military organizations offer incentives, increased salaries, flexible contract terms, and opportunities for career progression.

Fourth, there is a growing emphasis on multidisciplinary knowledge and collaborative training, incorporating a range of skills including cyber strategy, law, and information operations into officer education. For instance, programs like the three-week cybersecurity training at the German Marshall Center, which gathers officers from over 50 countries, exemplify this trend by addressing policy and cooperation challenges in the cyber domain.

To enhance personal cyber hygiene, international military organizations are now offering annual refresher training to all personnel, focusing on essential skills like data privacy, device usage, and password protection. In the United States, a system has been implemented where military personnel must pass an annual online exam and renew their network access privileges, effectively promoting personal accountability.

Therefore, cyber learning innovation is developing into a holistic system that integrates practical simulation, ongoing specialization, adaptable human resource practices, diverse knowledge from various fields, and personal discipline.

The practical implementation and effectiveness of the above trends are clearly demonstrated by the experience of foreign defense organizations. For instance, the United States established its Cyber Command in 2009 and, in 2018, granted it the status of an independent unified command, integrating cyber forces into the main structure of the armed forces. The country's cyber policy relies on public-private cooperation and has established coordination between the government, education, and technology sectors through real-world exercises such as the ISAC information exchange system and “Cyber Storm”. The use of the Stuxnet malware to damage Iran's nuclear facilities in cooperation with Israel in 2010 demonstrated the strategic use of cyber weapons, and the United States is currently pursuing a “Forward Offensive Cyber” or proactive defense strategy. In terms of human resources, although the Cyber Mission Force was established, stability issues led to the creation of the “Cyber Talent Management Organization” and “Advanced Training Center” in 2025, which began implementing continuous training and a flexible career system.

NATO has recently expanded its Cooperative Cyber Defense Center of Excellence (CCDCOE) in Estonia. The annual Locked Shields exercise provides member states with training for their red team/blue team teams in a realistic attack environment. This exercise is the largest practical simulation of decision-making at the command level and fosters the development of international cyber cooperation.

In Europe, countries such as Germany, the United Kingdom, and France are establishing academies and research institutes to train cyber officers. These programs offer a multidisciplinary approach that combines strategic, legal, and management knowledge with technical and tactical training.

Russia has integrated cyberspace into its defense policy as a strategic information warfare strategy. In 2012, it established a military academy under the Ministry of Defense to train officers in a program focused on "comprehensive information warfare." This program includes training in cyberattacks, information influence operations, psychological warfare, and counter-disinformation. A key aspect of Russian training is the principle of "defensive-offensive integration," which involves developing defensive and offensive capabilities simultaneously.

China views cyberspace as a crucial aspect of national security and has implemented a centralized cyber defense system under state control through the enactment of the "Network Security Law" in 2015. The Strategic Support Force of the People's Liberation Army is merging cyber, space, and electronic intelligence activities and is enhancing training and research focused on "integrated network warfare." Furthermore, academic institutions like Tsinghua and Harbin Engineering University are offering military programs to educate cyber officers and defense engineers, collaborating with public-private laboratories and innovation centers.

The experiences of the United States, NATO, Europe, Russia, and China demonstrate that cyber training is evolving into a strategic activity that is closely linked to political, defense policy, and technological advancements. It is developing into a comprehensive system that integrates ongoing human-focused training, practical training, collaborations between the public and private sectors, information warfare, and legal considerations.

Conclusions

Countries are constantly seeking the best ways to govern and organize themselves to enhance their cybersecurity. Some have restructured their existing frameworks (such as China's Strategic Support Force being disbanded and the US CYBERCOM being reorganized), showing that there is no universal model for cybersecurity governance. Instead, a flexible approach that addresses each country's unique circumstances and challenges is necessary. Due to reforms and investments made in the past decade, countries have significantly improved their cyber capabilities, which are now starting to influence the security landscape.

At the strategic level, the integration of cyberspace into national security strategies has helped define institutional responsibilities and has had a deterrent effect on an international scale. For instance, NATO's 2016 decision to consider cyber-attacks as a component of collective defense under Article 5 has prompted member states to incorporate cyber counterattack measures into their strategies, thereby reducing the motivation for carrying out such attacks.

At the operational level, the development and enhancement of cyber forces have significantly decreased the time required to identify and address attacks. The US swiftly detected the Solar Winds attack in 2020 and minimized the impact, while nations like Estonia and Finland are safeguarding their essential infrastructure through continuous monitoring systems.

Enhanced training at the tactical level is enhancing the cyber expertise of military personnel. For instance, within a US Air Force squadron, the percentage of personnel who were unaware of phishing emails in 2018 rose from 40% to 85% in 2021, primarily due to training. Cyber skills competitions in Estonia are promoting a culture of "ethical hacking" among cyber professionals and bolstering internal security resilience.

At the geopolitical level, cyber power has emerged as a new means of state influence and conflict. North Korea has generated significant profits through financial cyberattacks, a tactic often described as "warfare without actual warfare." In 2021, the US, EU, and NATO collaborated to levy sanctions against Chinese technology firms, leveraging cyber capabilities as a tool for diplomatic coercion.

Cyberspace reforms have ultimately enhanced national security and established a framework for monitoring cyber risks. However, this is a continuous effort, requiring readiness and staying ahead of evolving technology and new attack methods.

REFERENCES

1. Department of Defense. (2011). *Department of Defense strategy for operating in cyberspace*. U.S. Department of Defense. https://csrc.nist.gov/csrc/media/projects/ispab/documents/dod-strategy-for-operating-in-cyberspace.pdf
2. Costello, J., & McReynolds, J. (2018). *China's Strategic Support Force: A force for a new era* (China Strategic Perspectives No. 13). National Defense University Press. https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf
3. Giles, K. (2011). *"Information troops"- a Russian cyber command?* In C. Czosseck, R. Ottis, & K. Ziolkowski (Eds.), *Proceedings of the 3rd International Conference on Cyber Conflict*. NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/InformationTroopsARussianCyberCommand-Giles.pdf
4. Greenberg, A. (2018, August 22). The untold story of NotPetya, the most devastating cyberattack in history. *Wired*. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
5. Kania, E. B., & Costello, J. K. (2018). The strategic support force and the future of Chinese information operations. *Cyber Defense Review*, *3*(1), 105–124.
6. Lilly, B. (2022). *Russian information warfare: Assault on democracies in the cyber wild west*. U.S. Naval Institute Press.
7. Marshall Center. (n.d.). *Cybersecurity training programs*. George C. Marshall European Center for Security Studies. https://www.marshallcenter.org
8. Mongolia. (2021). *Cyber Security Law.* State Great Khural of Mongolia. https://legalinfo.mn/en/edtl/16531350476261
9. NATO Cooperative Cyber Defence Centre of Excellence. (2022). *Locked Shields exercise*. https://ccdcoe.org/exercises/locked-shields/
10. NATO Cooperative Cyber Defence Centre of Excellence. (2022.). *NATO Cooperative Cyber Defence Centre of Excellence*. https://ccdcoe.org/about-us/
11. NATO. (2021, January 18). NATO helps to strengthen Mongolia's cyber defence capacity. https://www.nato.int/cps/en/natohq/news_180697.htm
12. Spidalieri, F., & McArdle, J. (2016). Transforming the next generation of military leaders into cyber-strategic leaders: The role of cybersecurity education in US service academies. *The Cyber Defense Review*, *1*(1), 141–163. https://cyberdefensereview.army.mil/Portals/6/Documents/CDR%20Journal%20Articles/Transforming%20the%20Next%20Generation%20of%20Military%20Leaders_Spidalieri_McArdle.pdf
13. Tikk-Ringas, E., Kerttunen, M., & Spirito, C. (2014). Cyber security as a field of military education and study. *Joint Force Quarterly*, *75*, 57–60. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-75/jfq-75_57-60_Tikk-Ringas-et-al.pdf
14. U.S. Air Force Air University. (2012.). *Cyber warfare principles*. Air University. https://www.airuniversity.af.edu
15. U.S. Cyber Command. (2025.). *U.S. Cyber Command*. U.S. Department of Defense. https://www.cybercom.mil
16. U.K. Ministry of Defence. (2023.). *National Cyber Force*. Government of the United Kingdom. https://www.gov.uk/government/organisations/national-cyber-force